

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ «Тувинский государственный университет»
ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
КАФЕДРА МАТЕМАТИКИ И МЕТОДИКИ ПРЕПОДАВАНИЯ МАТЕМАТИКИ**

Выпускная квалификационная работа
(бакалаврская работа)

**Применение некоторых алгоритмов кодирования и
декодирования в практических задачах**

Работа допущена к защите

И.о.зав.кафедры _____

Танзы М.В., к.ф-м.н., доцент

(фамилия, и.о., должность, уч.степень и звание)

Работа защищена «__» _____ 20__ г.

С оценкой _____

Председатель ГЭК _____
(подпись)

Сенашов В.И. д.ф-м.н., профессор
ведущий научный сотрудник Института
вычислительного моделирования
СО РАН, Красноярск

Члены комиссии _____

(подписи)

Студентки 4 курса 5 группы

направление подготовки 01.03.01

профили «Математика»

очной формы обучения

Тулуш Аяна Андреевна
(Ф.И.О)

_____ (подпись)

«__» _____ 20__ г.

Научный руководитель: _____
(подпись)

Троякова Г.А., к.ф-м.н., доцент

(фамилия, и.о., должность, уч.степень и звание)

Кызыл – 2020.

Содержание:

Введение.....	3
Глава I.ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ИНФОРМАЦИИ»	
1.1.История возникновения теории кодирования и декодирования.....	6
1.2. Базовые понятия кодирования и декодирования.....	10
Глава II.ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ШИФРА ЦЕЗАРЯ	
2.1. Основные сведения о шифра Цезаря.....	14
2.2. Маршрутная транспортизация.....	16
2.3. Таблица Виженера.....	17
2.4. Модифицированный шифр Цезаря.....	18
ГЛАВА III . АВТОРСКИЕ ЗАДАЧИ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ЛИЧНОЙ ИНФОРМАЦИИ С ИСОЛЬЗОВАНИЕМ ШИФР ЦЕЗАРЯ	
3.1. Задачи с использованием метод сдвига.....	20
3.2. Задачи с использованием модифицированного шифра Цезаря.....	31
ЗАКЛЮЧЕНИЕ.....	35
СПИСОК ИСПОЛЬЗОВАННОЙ ИСТОЧНИКОВ.....	37

Введение

Теория кодирования — это раздел теории информации, изучающий способы отображения дискретных сообщений сигналами в виде определенных сочетаний символов.

Актуальность выпускной квалификационной работы состоит в том, что умение применять на практике результаты теории кодирования и декодирования в практических задачах. Для осуществления полноценного процесса передачи информации, при котором сам процесс должен успешно завершиться, а сообщение дойти от отправителя до получателя в полном объеме, который, в свою очередь, его правильно трактует, информацию необходимо закодировать.

В некоторых случаях возникает потребность засекречивания текста сообщения или документа, для того чтобы его не смогли прочитать, тем кому не положено. Для решения таких проблем мною были выбраны коды Цезаря (шифр Цезаря).

Для осуществления полноценного процесса передачи информации, при котором сам процесс должен успешно завершиться, а сообщение дойти от отправителя до получателя в полном объеме, которое, в свою очередь, его правильно трактует, необходимо закодировать.

Сегодня для передачи и отображения информации мы используем вычислительную технику, которая «не понимает» наш язык без специальных операций — кодирования и декодирования.

Прежде чем разобраться с основами процедуры кодирования, следует ознакомиться с несколькими простейшими понятиями.

Задача кодирования — это задача перевода дискретного сообщения из одного алфавита в другой. Причем такое преобразование не должно приводить к потере информации.

Цели кодирования заключаются в доведении идеи отправителя до получателя, обеспечении такой интерпретации полученной информации получателем, которая соответствует замыслу отправителя. Для этого

используются специальные системы кодов, состоящие из символов и знаков. Код представляет собой систему условных знаков (символов), предназначенных для представления информации по определенным правилам. В настоящее время понятие «код» трактуется по-разному.

Объектом исследования является процесс обучения применению некоторых алгоритмов кодирования и декодирования .

Предметом исследования является применения некоторых алгоритмов кодирования и декодирования.

Целью исследования является применение некоторых алгоритмов кодирования и декодирования в практических задачах.

Теоретической основой выпускной аттестационной работы стали исследования [ученых](#) по разделу кодирования и декодирования информации , и по [шифрованию Цезаря](#). Теоретические основы использования кодирования и декодирования в личной информации представлены также в работах А.И.Митюхин, Ю.Н.Мальцев , А.Д.Поспелов , С.Г.Колесников, Ф.И.Соловьева, А.В.Косточка.

Структура работы. Работа состоит из введения, трех глав , заключения , списка использованной литературы.

Во введении обосновывается актуальность выбранной темы , формируется цель, предмет и объект исследования , определяются теоретические основы выпускной квалификационной работы, раскрывается структура исследования.

В первой главе «Теоретические основы кодирования и декодирования информации» рассматривается история возникновения кодирования и декодирования информации и базовые понятия.

Во второй главе «Теоретические основы шифра Цезаря» рассматривается история возникновения шифра Цезаря и основные понятия шифра Цезаря.

В третьей главе составляются авторские задачи кодирования и декодирования личной информации с использованием шифр Цезаря.

В заключении формулируются основные выводы и предложения, сделанные на основе проведенных исследований, суть которых изложена в отдельных главах данной выпускной квалификационной работы.

Глава I .ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ИНФОРМАЦИИ»

1.1.История возникновения теории кодирования и декодирования

Теория кодирования — это раздел теории информации, изучающий способы отображения дискретных сообщений сигналами в виде определенных сочетаний символов.

С глубокой древности люди искали эффективные способы передачи информации:

- Движение факелов использовал древнегреческий историк Полибий (II в. До н.э.);



Рис.1 Схема кодирования букв греческого алфавита с помощью двух групп факелов.

- Оптический телеграф – семафор – впервые использовал

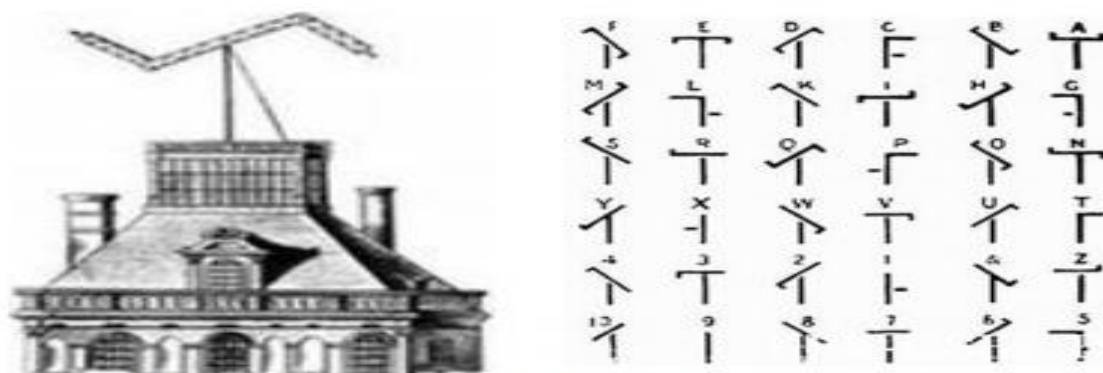
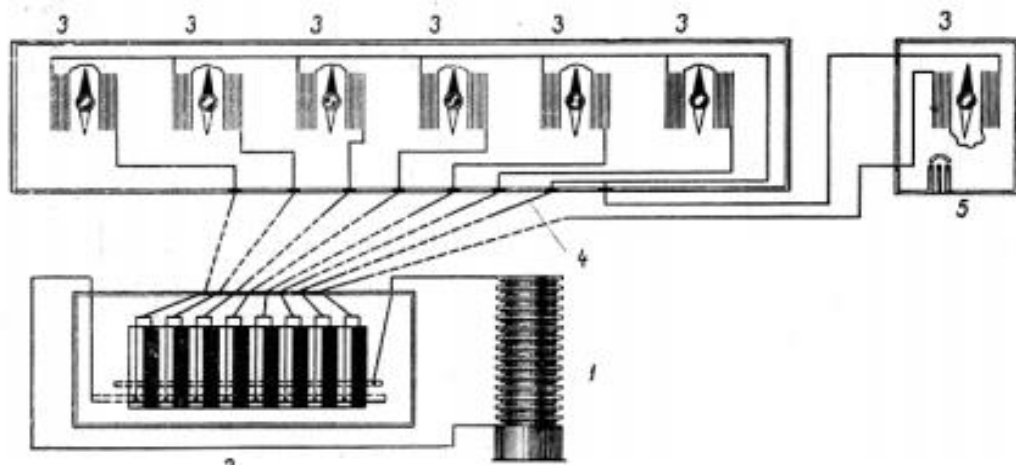


Рис.2 Оптический семафор К.Шатта и его телеграфный алфавит.

- Движение электромагнитной стрелки в электромагнитных телеграфных аппаратах впервые применили русский физик П.Л. Шиллинг (1832) и профессора Гёттинггенского университета Вебер и Гаусс (1833);



*Рис.3 Схема электромагнитного телеграфа П.Л.Шиллинга
(1 — источник тока, 2 — клавиатура, 3 — магнитные стрелки,
4 — провод обратной связи, 5 — вызывное устройство)*

- Азбука и телеграфный аппарат Самюэла Морзе (1837);

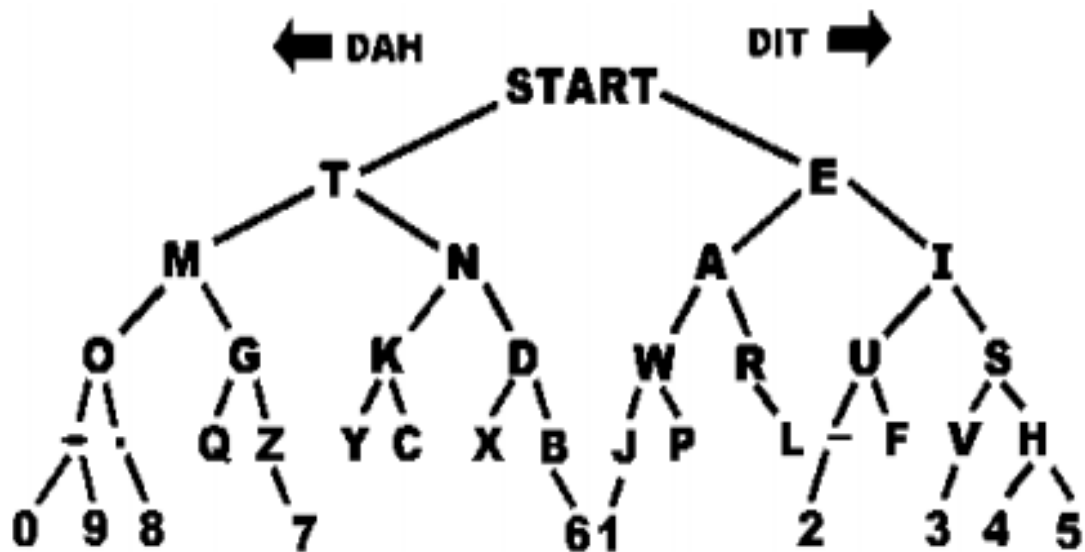


Рис. 4 Дерево кода Морзе - направо точка, налево тире.

- Международный флажковый код для передачи информации оптическими сигналами впервые ввел капитан Фредерик Марьят в 1861 г. на основе свода корабельных сигналов;



Рис.5 Морская азбука сигнальных флажков

- Беспроволочный телеграф (радиопередатчик) был изобретен А.С.Поповым в 1895 г. И Маркони в 1897 г. независимо друг от друга;

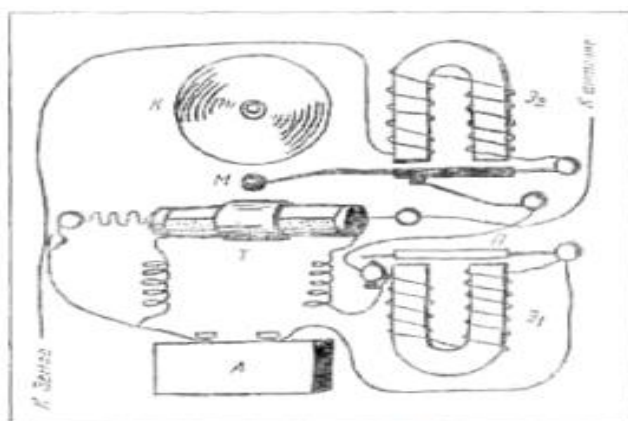


Рис.6а Схема прибора Попова: Т — трубочка с железными опилками; К — колокол звонка; М — молоточек; А — аккумулятор, подающий ток в трубочку с опилками; Э1 и Э2 — электромагниты; П — железная пластинка.

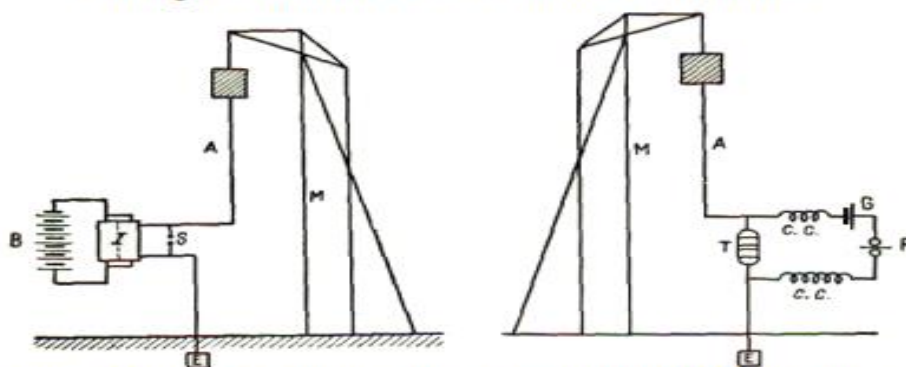


Рис. 6б Схема беспроводного телеграфа Маркони. Слева

- Беспроволочный телефон, телевидение (1935), затем и ЭВМ – новые средства связи, появившиеся в XX в., с которыми связана новая эпоха в информатизации общества.

Одновременно с потребностью передавать информацию люди искали способы скрыть смысл передаваемых сообщений от посторонних любопытных глаз. Императоры, торговцы, политики и шпионы искали способы шифрования своих посланий. Образцы тайнописи можно встретить еще у Геродота (V в. до н. э.). К тайнописи – криптографии прибегал Гай Юлий Цезарь, заменяя в своих тайных записях одни буквы другими. Использовали шифрование не только древнегреческие жрецы, но и ученые Средневековья: математики итальянец Джероламо Кардано и француз Франсуа Виет, нидерландский гуманист, историк, юрист Гроций, выдающийся английский философ Фрэнсис Бэкон. Отцом криптографии считается архитектор Леон Баттиста Альберти (1404-1472), который ввел шифрующие коды и многоалфавитные подстановки. [1,с.45]

Сэр Фрэнсис Бэкон (1561 – 1626), автор двухлитерного кода, доказал в 1580 г., что для передачи информации достаточно двух знаков. Также Ф.Бэкон сформулировал требования к шифру:

1. Шифр должен быть несложен, прост в работе;
2. Шифр должен быть надежен, труден для дешифровки посторонним;
3. Шифр должен быть скрытен, по возможности не должен вызывать подозрений.

Шифры Бэкона – сочетание шифрованного текста с дезинформацией в виде нулей. Таким образом, двузначные коды и шифры использовались задолго до появления ЭВМ.

Новый толчок развитию теории кодирования дало создание в 1948 году Клодом Эльвудом Шенноном (1916 — 2001) теории информации. Идеи, изложенные Шенноном в статье «Математическая теория связи», легли в основу современных теорий и техник обработки, передачи и хранения информации. Результаты его научных исследований способствовали

развитию помехоустойчивого кодирования и простых методов декодирования сообщений.

2.2. Базовые понятия кодирования и декодирования.

Сегодня для передачи и отображения информации мы используем вычислительную технику, которая «не понимает» наш язык без специальных операций – кодирования и декодирования.

Прежде чем разобраться с основами процедуры кодирования, следует ознакомиться с несколькими простейшими понятиями.

Задача кодирования – это задача перевода дискретного сообщения из одного алфавита в другой. Причем такое преобразование не должно приводить к потере информации. Алфавит, с помощью которого представляется информация до преобразования называется первичным, а алфавит конечного представления – вторичным.

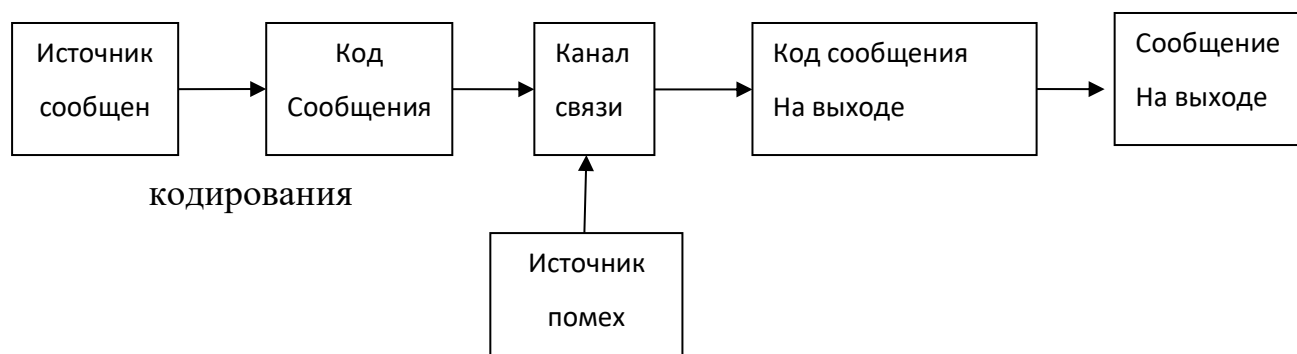
При определении понятия «код» используют два подхода. С одной стороны, **код — это правило**, описывающее соответствие знаков или их сочетаний первичного (исходного) алфавита знакам или их сочетаниям вторичного алфавита. Также кодом называют **набор знаков** вторичного алфавита, используемый для представления знаков или их сочетаний первичного алфавита.

Код – это набор любых символов или других визуальных обозначений информации, который образует представление данных. В *компьютерной технике* под кодом подразумевают отдельную систему знаков, которые используют для обработки, передачи и хранения сообщений и файлов.

Кодер – устройство, обеспечивающее выполнение операции кодирования.[2,с.15]

Кодирования информации – процесс преобразование сигнала из формы, удобный для непосредственного использования информации , в

форму , удобную для передачи , хранения или автоматической переработки. Много вопросов о кодировании возникает при передаче сообщений. Они могут быть проиллюстрированы приводимой здесь схемой



Поясним термины , встречающиеся в данной схеме. Обозначим через α алфавит , состоящий из конечного числа букв , через $S(\alpha)$ – множество слов в алфавите α , а через $S'(\alpha)$ – некоторое подмножество слов из $S(\alpha)$.

Объект , порождающий слово из $S'(\alpha)$, называется источником сообщений , а слова из $S'(\alpha)$ – сообщениями . Существует несколько способов описания источника сообщений. Основными способами являются теоретико-множественный , при котором фиксируются мощностные характеристики источника сообщений; статистический , когда, например, задаются вероятности появления каждой буквы ; логический , который характеризует способы построения слова.

Канал связи можно рассматривать как устройство с одним входом и с одним выходом. На вход этого устройства поступает код сообщения V , на выходе получают код сообщения V' , где V' - слово в некотором алфавите β' . В простейшем случае , когда канал связи тождественный , $\beta = \beta'$, $V = V'$.

Источник помех вносит ошибки в канал связи, вызывая искажения кодов на выходе. Для его описания используют два способа: логико-комбинаторный, связанный с указанием ограничений на число единичных ошибок, и статистический. Который заключается в указании вероятностных характеристик источника.

Коррекция и декодирования

Способы кодирования информации бывают различные и зависят они, в первую очередь, от целей кодирования.

Наиболее распространенными из которых являются:

- экономность (достигается сокращением записи);
- надежность (информацию необходимо засекретить таким образом, чтобы она была недоступна третьим лицам);
- с удобством передачи кодов;
- со стремлением увеличить пропускную способность канала;
- с удобством обработки кодов;
- с обеспечением помехоустойчивости;
- удобство обработки или восприятия.

Чаще всего кодированию подвергаются тексты на естественных языках (русском, английском и пр.).

Цели кодирования заключаются в доведении идеи отправителя до получателя, обеспечении такой интерпретации полученной информации получателем, которая соответствует замыслу отправителя. Для этого используются специальные системы кодов, состоящие из символов и знаков. Код представляет собой систему условных знаков (символов), предназначенных для представления информации по определенным правилам. В настоящее время понятие «код» трактуется по-разному.

В процессах восприятия , передачи и хранения информации живыми организмами , человеком и техническими устройствами происходит кодирование информации .В этом случае информация , представленная в одной знаковой системе , преобразуется в другую. Каждый символ исходного алфавита представляется конечной последовательностью символов кодового алфавита. Эта результирующая последовательность называется информационным кодом (кодовым словом , или просто кодом).

Преобразование знаков или групп знаков одной знаковой системы в знаки или группы знаков другой знаковой системы называется **перекодированием.**

При кодировании один символ исходного сообщения может заменяться одним или несколькими символами нового кода, и наоборот — несколько символов исходного сообщения могут быть заменены одним символом в новом коде. Примером такой замены служат китайские иероглифы, которые обозначают целые слова и понятия.[5,с.250]

Ниже рассматриваются два вида кодирования:

(а) Алфавитное кодирование. Каждой букве a_i из $A = \{a_1, \dots, a_r\}$ ставится в соответствие некоторое слово B_i из алфавита $B = \{b_1, \dots, b_q\}$. Схема кодирования, сопоставляющая эти слова, будет обозначаться буквой Σ .

(б) Равномерное кодирование. Некоторое слово B_i из алфавита B ставится в соответствие не букве, а какому-то слову A_i фиксированной длины в алфавите A . Конечно, одно из первых требований к используемому коду — требование однозначности восстановления сообщения по его коду.

Декодер — устройство, производящее декодирование.

Декодирования информации — обратный процесс восстановления информации из закодированного представления.[3,с.32]

В зависимости от системы кодирования информационный код может или не может быть декодирован однозначно. Равномерные коды всегда могут быть декодированы однозначно.

Для однозначного декодирования неравномерного кода важно, имеются ли в нем кодовые слова, которые являются одновременно началом других, более длинных кодовых слов.

Закодированное сообщение можно однозначно декодировать с начала, если выполняется **условие Фано**: никакое кодовое слово не является началом другого кодового слова.

Закодированное сообщение можно однозначно декодировать с конца, если выполняется обратное условие Фано: никакое кодовое слово не является окончанием другого кодового слова.

Глава II. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ШИФРА ЦЕЗАРЯ.

2.1. Основные сведения о шифре Цезаря.

Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского полководца Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами. [7, с.28]

В криптографии древних времен использовались два вида шифров: замена и перестановка. Наиболее древним и распространённым примером шифра замены является шифр Цезаря. Гай Юлий Цезарь использовал в своей переписке шифр собственного изобретения. Суть шифра Цезаря состоит в том, что буквы алфавита заменяются буквами того же алфавита, но со сдвигом вправо на 3 позиции. Пример ключа применительно к русскому языку будет выглядеть так:

Открытый текст:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э
Ю Я

Зашифрованный:

Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б
В

При зашифровывании буква А заменялась буквой Г, Б заменялась на Д, В — Е и так далее. Так, например, «РИМ» превращалось в слово «УЛП». Получатель сообщения «УЛП» искал эти буквы в нижней строке и по буквам над ними восстанавливал исходное слово «РИМ». Ключом в шифре Цезаря является величина сдвига 2-ой нижней строки алфавита, в нашем случае это

число 3. Преемник Юлия Цезаря – Цезарь Август использовал тот же шифр, но с ключом – сдвиг 1. Слово «РИМ» в этом случае зашифровывается, как «СЙН».

Развитие шифра Цезаря весьма очевидно, так как в нижней строке двухстрочной записи буквы алфавита могут быть расположены в произвольном порядке. Применительно к русскому языку в нижней строке существует всего 33 варианта ключей (число букв в русском алфавите), при их произвольном расположении число ключей становится огромным. Оно равно $33!$ (33 факториал), т. е. приблизительно десять в тридцать пятой степени. Это важный момент. Если противник узнал или догадался об используемом шифре, то он может попытаться расшифровать текст путём полного перебора ключей. Даже в современных условиях это занимает большое количество времени и ресурсов, что уж говорить о тех древних временах, когда из-за повсеместной неграмотности населения, не представлялась возможность за зашифрованным текстом увидеть свой язык. Многие люди, видя шифр, считали, что запись сделана на иностранном языке. [10,с.46]

В художественной литературе классическим примером шифра замены является известный шифр «Пляшущие человечки» К. Дойля. В нём буквы заменялись на символические фигурки людей. Ключом такого шифра являлись позы человечков, заменяющих буквы. Фрагмент зашифрованного послания представлен на рисунке 7:



Рисунок 7. Фрагмент зашифрованного послания.

Для получения соответствующего закрытого текста использован шифр простой замены букв на фигурки людей; флажок в руках означает конец слова, таким образом, эти пляшущие человечки с флажками могли шифровать огромный набор данных. Криптографическая стойкость такого шифра даже в те времена была не особо высокой, ведь пользуясь статистическими знаниями при написании слов, мы можем с легкостью отличить наиболее часто повторяющиеся гласные буквы, что существенно облегчит перебор возможных вариантов.[8,с.87]

2.2. Маршрутная транспозиция.

К классу перестановки относится шифр маршрутная транспозиция и его вариант постолбцовая транспозиция. В каждом из них в данный прямоугольник $[n \times m]$ сообщение вписывается заранее обусловленным способом, а столбцы нумеруются или обычным порядком следования, или в порядке следования букв ключа – буквенного ключевого слов.

Термин “шифр” арабского происхождения. В начале XV в. Арабы опубликовали энциклопедию “Шауба Аль-Аща”, в которой есть специальный раздел о шифрах. В этой энциклопедии указан способ раскрытия шифра простой замены. Он основан на различной частоте повторяемости букв в тексте. В этом разделе есть перечень букв в порядке их повторяемости на основе изучения текста Корана. Заметим, что в русском тексте чаще всего встречается буква “О”, затем буква “Е” и на третьем месте стоят буквы “И” и “А”. Более точно: на 1000 букв русского текста в среднем приходится 90 букв “О”, 72 буквы “Е” или “Ё”, 60 букв “И” и “А” и т.д. [11,с.20]

Неудобство шифров типа подстановка (простая замена) в случае использования стандартного алфавита очевидно. Таблица частот встречаемости букв алфавита позволяет определить одни или несколько символов, а этого иногда достаточно для дешифрования всего сообщения (“Пляшущие человечки” Конан Дойля или “Золотой жук” Эдгара По). Поэтому обычно пользуются разными приемами, чтобы затруднить

дешифрование. Для этой цели используют многобуквенную систему шифрования – систему, в которой одному символу отвечает одна или несколько комбинаций двух и более символов. Другой прием – использование нескольких алфавитов. В этом случае для каждого символа употребляют тот или иной алфавит в зависимости от ключа, который связан каким-нибудь способом с самим символом или с его порядком в передаваемом сообщении.[9,с.5]

2.3. Таблица Виженера.

В процессе шифрования (и дешифрования) используется таблица Виженера, которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой равно числу столбцов в алфавите. Чтобы зашифровать какое-нибудь сообщение, поступают следующим образом. Выбирается слово – лозунг и подписывается с повторением над буквами сообщения.

Чтобы получить зашифрованный текст, находят очередной знак лозунга, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном.

Пример 1. Таблица 1, составлена из 31 буквы русского алфавита (без букв Ё и Ъ). Выбираем лозунг – математика. Находим столбец, отвечающий букве "м" лозунга, а затем строку, соответствующую букве "к". На пересечении выделенных столбца и строки находим букву "ц". Так продолжая дальше, находим весь зашифрованный текст.

м а т е м а т и к а м а т е м а т и к а м а т е м а
к р и п т о г р а ф и я с е р ь е з н а я н а у к а

Таблица 1.

А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я
Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А
В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б
Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В
Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г
Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д
Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е
И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З
Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З
Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И
К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й
Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К
М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л
Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М
О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н
П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О
Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П
С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р
Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С
У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т
Ф Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У
Х Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф
Ц Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х
Ч Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц
Ш Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч
Щ Ъ Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш
Ь Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ
Ы Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ
Э Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы
Ю Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э
Я А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Э Ю

ц р ь ф я о х ш к ф ф я д к э ь ч п ч а л н т ш ц а ♦

Наконец , к сообщению можно применять несколько систем шифрования.[12,с.83]

2.4.Модифицированный шифр Цезаря.

Аббат Тритемеус – автор первой печатной книги о тайнописи (1518г.) – предложил несколько шифров и среди них шифр, который можно считать

усовершенствованием шифра Цезаря. Этот шифр устроен так. Все буквы алфавита нумеруются по порядку (от 1 до 31 в русском варианте). Затем выбирают какое-нибудь слово, называемое "ключом", и подписывают под сообщением с повторением.

Чтобы получить зашифрованный текст, складывают номер очередной буквы с номером соответствующей буквы ключа. Если полученная сумма больше 31, то из нее вычитают 31. В результате получают последовательность чисел от 1 до 31. Вновь заменяя числа этой последовательности соответствующими буквами, получают зашифрованный текст. Разбиваем этот текст на группы одной длины, получают зашифрованное сообщение. [6, с.11]

Пример 2. Выбираем ключевое слово "Пособие". Составляем сообщение "сессия начинается в конце семестра"

с
с
е
с
с
и
я
н
а
ч
и
н
а
е
т
с
я
в
к
о
н
ц
е
с
е
м
е
с
т
р
а

п
о
с
о
б
и
е
п
о
с
о
б
и
е
п
о
с
о
б
и
е
п
о

Шифруем, разбиваем текст на группы длины 6, и получаем зашифрованное сообщение:

в ф д а и и у р з ь э в о ш в о ф щ р ц э х б ч ы з ь ш б п ♦

Чтобы получить зашифрованный текст, складывают номер очередной буквы с номером соответствующей буквы ключа. Если полученная сумма больше 33, то из нее вычитают 33. В результате получают последовательность чисел от 1 до 33. Вновь заменяя числа этой последовательности соответствующими буквами, получают зашифрованный текст. Разбивал этот текст на группы одной длины (например, по 5), получают зашифрованное сообщение.

Если под ключом шифра понимать однобуквенное слово "В" (в русском варианте), то мы получим шифр Цезаря.

ГЛАВА III. АВТОРСКИЕ ЗАДАЧИ КОДИРОВАНИЯ И ДЕКОДИРОВАНИЯ ЛИЧНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ ШИФРА ЦЕЗАРЯ.

3.1. Задачи с использованием метода сдвига.

Задача 1. Шифрование с использованием ключа $k=3$. Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее:

Исходный алфавит:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифрованный:

Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

Оригинальный текст :

Заключение.

Дано Богомоловой Ольге Олеговне , зарегистрированной : г.Кызыл , ул.Калинина,10, в том , что она осмотрена врачом психиатром высшей категории к.м.н. Соколова.А.С. На момент осмотра расстройств психотического уровня , показаний к госпитализации в психиатрический стационар не выявлено.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

Кгнобъзрлз.

Жгрс Дсёслсосесм Солёз Созёсерз, кгрзёлфхрлрсегррсм : ё.Нюкюо, цо Нголрлрг , 10 , е хсл, тхс срг сфпсхузрг еугъсп-тфлшпгхуп еюфым нгхзёсулл н.п.р. Фенсосег.Г.Ф. Рг пспзрх сфпсхуг угффхусмффхе тфлшсхлъзфнсёс цусерв, тенгкгрлм н ёсфлтлхгокгщлл е тфлшлгхульзфлм фхгщлсрги рз еювеозрс.

Задача 2. Шифрование с использованием ключа $k=1$. Буква «Е» «сдвигается» на одну букву вперёд и становится буквой «Ё». Твёрдый знак, становится буквой «І», и так далее:

Выписка из истории болезни.

Иргит Аржаан, находится в детском онко-гематологическом отделении больницы №1 с 03 апреля 2019г. с диагнозом:

Эмбриональная рабдомиосаркома с поражением мягких тканей полостей носа, основной и левой верхне-челюстной пазух, с частичным разрушением стенок основной пазухи, костей решетчатого лабиринта, разрушением костной стенки передней черепной ямки слева.

Диагноз поставлен на основании клинических данных – отсутствие носового дыхания, результатов КТ околоносовых пазух с 01 марта 2019г. и МРТ от 9 марта 2019г.

Гистологически и иммуногистохимически от 05 апреля 2019г. – Эмбриональная рабдомиосаркома. Больной нуждается в интенсивной полихимиотерапии по протоколу CWS-2002.

Шифрованный текст:

Гърйтлб йи йтупсйй впмёиой.

Йсдйу Бсзббо, общейута г еёутлпн полп-дёнбубмпдйшётлпн пуюёмёой впмэойч №1 т 03 брсёма 2019д. т ейбдопиин:

Юнвсйпобмэоба сбвепнийтбслпнб т рпсбзёойён надлиц улбоёк рпмптуёк оптб, птопгопк й мёгпк гёсцоё-шёмятуопк рбифц, т шбтуйшоён сбисфщёойён туёопл птопгопк рбифцй, лптуёк сёщёушбупдп мбвйсийоуб, сбисфщёойён лптуопк туёоли рёсёеоек шёсёропк анлий тмёгб

Ейбдопи рптубгмёо об птопгбойй лмйойшётлийц ебооыц – путфутугйё оптпгпдп еыцбойа, сёифмэубупг ЛУ плпмпоптпгыц рбифц т 01 нбсуб 2019д. й НСУ пу 9 нбсуб 2019д.

Дйтупмпдйшётлий й йннфопдйтупцийнйшётлий пу 05 брсёма 2019д. – Юнвсйпобмэоба сбвепнийтбслпнб. Впмэопк офзебёута г йоуёотйгопк рпмйцийнйпуёсбрий рп рспуплпмф CWS-2002.

Задача 3. Шифрование с использованием ключа $k=4$. Буква «Е» «сдвигается» на четыре букв вперёд и становится буквой «И». Твёрдый знак, перемещённый на четыре буквы вперёд, становится буквой «Ю», и так далее:

Выписной эпикриз из медицинской карты стационарного больного.

Ребёнок Громова Владислава Вадимовна 28.06.2012. находился на стационарном лечении Республиканской детской клинической больницы №3 неврологическом отделении с 06.10.2015г. по 01.11.2015г. с клиническим диагнозом : ДЦП , спастическая диплегия , средней тяжести. Задержка психоречевого развития.

Сопутствующий диагноз : Первичное содружественное с паралитическим компонентом сходящееся косоглазие . Спастические эквинусные стопы.

Жалобы при поступлении : на задержку психоречевого и моторного развития.

Девочка больная с рождения , в анамнезе перинатальная патология : гестоз , недоношенность 1-2 степени, родилась при сроке беременности 28-29 недель, вес при рождении 950г, гипоксия ЦНС. Состояние при рождении тяжелое. Развивается с задержкой : голову стала держать в 4 месяце , сидеть в 11 месяцев.

Неврологический статус : окружность головы 47 см, в контакт вступает, речевая активность на уровне отдельных слов , запас слов ограничен. ЧМН – сходящееся косоглазие . Двигательная сфера – стоит и ходит при поддержке, опора на носочках . Мышечный тонус в руках и ногах высокий , грубее в ногах. Сухожильные рефлексы оживлены. Отмечаются приводящие контрактуры в тазобедренных суставах , спастические эквинусные стопы.

Проведено обследование:

ОАМ в норме ; кал на я/г отр.

Логопед : Задержка психоречевого развития.

Психолог : Признаки задержки психоречевого развития.

ЭЭГ : умеренные изменения электрической активности мозга , дисфункция срединных структур мозга.

Ортопед : Спастические эквинусные стопы.

Окулист : DS первичное содружественное сходящееся косоглазие с паралитическим компонентом.

УЗИ органов брюшной полости : реактивные изменения парасимы печени , 2-х сторонний хронический пиелонефрит.

Эндокринолог : эндокринный патологии не выявлено.

Проведено лечение : массаж , физиолечение – озонотерапия , электрофорез с эуфилином на шейный отдел позвоночника иглорефлексотерапия , актовегин , циннаризин , танакан , мидокалы , витамины B6,B12, пирацетам.

Выписывается с улучшением : уменьшился гипертонус ,увеличился объем активных движений.

Рекомендовано :

1. ЛФК – регулярно
2. Нейтротрофит по ¼ табл. 1 раз в день 1 месяц
3. Фолиевая кислота по ½ таб. 2 раза в день 1 месяц

Повторный курс лечения через 6 месяца.

Шифрованный текст:

Ёяумхстн бумофмл мл ризмъмсхотн одфця хцдъмтсдфстжт етпастжт.
Фиейсто Жфтртёд Ёпдзмхпдёд Ёдзмртёсд 28.06.2012. сдштзмпахг сд
хцдъмтсдфстр пиыисмм Фихучепмодсхотн зицхотн опмсмыихотн етпасмъи
№3 сиёфтптжмыихотр тцзиписмм х 06.10.2015ж. ут 01.11.2015ж. х
опмсмыихомр змджстлтр : ЗЪУ , худхцмыиходг змупижмг , хфизсин
цгкихцм. Лдзифкод ухмштфийиётжт фдлёмцмг.

Хтучцхцёчвэмн змджстл : Уифёмысти хтзфчкихцёиссти х
удфдпмцмыихомр отрутсисцтр хштзгэиыхг отхтжпдлми . Худхцмыихоми
боёмсчхсяи хцтуя.

Кдптея уфм утхцчуписмм : сд лдзифкоч ухмщтфиийётр м ртцтфстр
фдлёмцмм.

Зиётюд етпасдг х фткзисмг , ё дсдрсили уифмсдцдпасдг удцтптжмг :
жихцтл , сизтстысстхца 1-2 хциуисм, фтзмдха уфм хфтои еифирисстхцм
28-29 сизипа, ёих уфм фткзисмм 950ж, жмутохмг ЪСХ. Хтхцтгсми уфм
фткзисмм цгкипти. Фдлёмёдицхг х лдзифкотн : жтптёч хцдпд зифкдца ё 4
рихгьи , хмзица ё 11 рихгьиё.

Сиёфтптжмыхомн хцдцх : тофчкстхца жтптёя 47 хр, ё отсцдоц
ёхцчудиц, фиыйёдг доцмёстхца сд чфтёси тцзипасящ хптё , лдудх хптё
тжфдсмыис. ЫРС – хцтзгэиыхг отхтжпдлми . Зёмждципасдг хшифд – хцтмц
м щтзмц уфм утзифкои, тутфд сд стхтыюдщ . Ряьиысян цтсчх ё фчодщ м
стждщ ёяхтомн , жфчеии ё стждщ. Хцщткмпасяи фишпиохя ткмёпися.
Тцриыдвцхг уфмётзгэми отсцфдоцчфя ё цдлтеизфиссящ хчхцдёдщ ,
худхцмыхоми боёмсчхсяи хцтуя.

Фхужийту уёцрйиужетнй:

УЕС ж тухсй ; пер те д/з учх.

Рузуфйи : Меййхлпе фцнъухйьйжузу хемжнчнд.

Фцнъуруз : Фхнмтепн меййхлпн фцнъухйьйжузу хемжнчнд.

ВВЗ : шсйхйттай нмсйтйтнд врипчхныйцпуо епчнжтуцн сумзе ,
инцщштпынд цхийингтаъ цчхшпчшх сумзе.

Ухчуфйи : Цфецчныйцпнй впжнтшцтай цчуфа.

Упшрнцч : DS фйхжньтуй цуихйлийцжйттуй цъуидюйцд пуцузремнй ц
фехернчныйцпнс пусфутйтчус.

ЧЛМ тфждетё ефвьстн утптхцм : фидоцмёсяи млрисисмг удфхмщмря
уиыисм , 2-щ хцтфтссмн щфтсмыхомн умхптсишфмц.

Бсзтофмсптж : бсзтофмсеян удцтптжмм си ёягёпист.

Уфтёизист пиыисми : рдххдк , шмлмтпиыисми – тлиоифмцтёяи
дуупмодьмн , бпиоцфтштфил х бчшмпмстр сд ынсян тцзип утлётстысмод

мжптфишпиохтцифдумг , доцтёижмс , ъмссдфмлмс , цдсдодс , рмзтодпя , ёмцдрмся Ё6,Ё12, умфдъицдр.

Ёяумхяёдицхг х чпчыьисмир : чрисаьмпхг жмуифцтсчх ,чёипмымпхг теюир доцмёсяц зёмкисмн.

Фиотмисзтёдст :

1. ПШО – фижчпгфст
 2. Синцфтрчацмёмц ут $\frac{1}{4}$ цдеп. 1 фдл ё зиса 1 рихгъ
 3. Штпмиёдг омхптцд ут $\frac{1}{2}$ цде. 2 фдлд ё зиса 1 рихгъ
- Утёцтфсян очфх пиыисмг ыифил 6 рихгъд

Задача 4. Шифрование с использованием ключа $k=5$. Буква «Е» «сдвигается» на пять букв вперёд и становится буквой «Й». Твёрдый знак, перемещённый на пять буквы вперёд, становится буквой «Я», и так далее:

Оригинальный текст :

Логины и пароли студентов ФМФ 4 курса 5 группы для дистанционного обучения

логин	Пароль	фамилия имя отчество
Mat1801	ОНАУХ01	Ондар Наталья Александровна
Mat1802	САВК02	Самбала Айрана Витальевна
Mat1803	САМО03	Сат Аюша Монгун-ооловна
Mat1804	СЧЮЧХ04	Сундуй Чимис Юрьевна
Mat1805	ТААСХ05	Тулуш Аяна Андреевна
Mat1806	ТААЧХ06	Тюлюш Ай-Суу Артёмовна
Mat1807	ЧНЮКХ07	Чаш-оол Надежда Юрьевна
Mat1808	ШАРЧХ08	Шунней Айжана Радиевна
Mat1809	ХМСПХ09	Хертек Мерген Сарыг-оолович

Шифрованный текст:

Рузнта н фехурн ццшийтчуж ЩСЩ 4 пшхце 5 зхшффа ирд инцетынуттузу у
ёшьйтнд

рузнт	Фехурб	Щеснрнд нсд учыйцижу
Сеч1801	УТЕШЪ01	Утиех Течербд Ерыпцетихужте
Сеч1802	ЦЕЖП02	Цесёере Еохете Жнчербйжте
Сеч1803	ЦЕСУ03	Цеч Егэе Сумзшт-ууружте
Сеч1804	УЫГЪ04	Цштишо Ынснц Гхбйжте
Сеч1805	ЧЕЕЦЪ05	Чшршэ Едте Етихийжте
Сеч1806	ЧЕЕЪ06	Чгргэ Ео-Цшш Ехсйсужте
Сеч1807	ЫТГПЪ07	Беэ-уур Теийлие Гхбйжте
Сеч1808	ЭЕХЪ08	Эшттийо Еолете Хеинйжте
Сеч1809	ЪСЦФЪ09	Ъйхчийп Сйхзйт Цехаз-ууружнь

Задача 5. Шифрование с использованием ключа $k=8$. Буква «Е» «сдвигается» на восемь букв вперёд и становится буквой «М». Твёрдый знак, перемещённый на восемь буквы вперёд, становится буквой «В», и так далее:
Оригинальный текст :

Выписка из лицевого счёта.

1. Материальная помощь из стипендиального фонда +3480
2. Комиссия за СМС сообщение по счёту -59
3. Ежемесячное пособие на детей за март +192
4. Перевод денежных средств за услуги «Сотового – Теле 2» в пользу Теле 2 через АО «Киви- банк» -500
5. Комиссия банка за приём перевода в пользу Теле 2 через АО «Киви – Банк» -5
6. РУС , РСХБ интернет банк ДБО Трансфер +9000
7. РУС, АТМ 9265 Дружба 21в -10000
8. Перевод денежных средств за услуги «Сотового – Мегафон» в пользу Мегафон через АО «Киви- банк» -600
9. Комиссия банка за приём перевода в пользу Мегафон через АО «Киви – Банк» -6
10. РУС, АТМ 8466 Кочетова 1 -10000

Шифрованный текст:

Йгчрщтз рп урюмйцкц щяньз.

1. Фзъмшрзудхзж чцфцбд рп щърчмхлрзудхцкц ыцхлз +3480
2. Тцфрщщрж пз ЩФЩ щццибмхрм чц щяньы -59
3. Момфмщжяхцм чцщцирм хз лмъмс пз фзшь +192
4. Чмшмйцл лмхмохгэ щшмлщъй пз ыщуыкр «Щцъйцкц – Ъмум 2» й чцудпы Ъмум 2 ямшмп ЗЦ «Трйр- изхт» -500
5. Тцфрщщрж изхтз пз чшрнф чмшмйцлз й чцудпы Ъмум 2 ямшмп ЗЦ «Трйр – Изхт» -5
6. ШЫЩ , ШЦЭИ рхъмшхмъ изхт ЛИЦ Ъшзхщъмш +9000
7. ШЫЩ, ЗЪФ 9265 Лшыоиз 21й -10000
8. Чмшмйцл лмхмохгэ щшмлщъй пз ыщуыкр «Щцъйцкц – Фмкзыцш» й чцудпы Фмкзыцх ямшмп ЗЦ «Трйр- изхт» -600
9. Тцфрщщрж изхтз пз чшрнф чмшмйцлз й чцудпы Фмкзыцх ямшмп ЗЦ «Трйр – Изхт» -6
10. ШЫЩ, ЗЪФ 8466 Тцямъцйз 1 -10000

Задача 6. Шифрование с использованием ключа $k=12$. Буква «Е» «сдвигается» на двенадцать букв вперёд и становится буквой «Р». Твёрдый знак, перемещённый на двенадцать буквы вперёд, становится буквой «Ё», и так далее:

Оригинальный текст :

Письмо из фронта Терентия Ивановича Шнырова.

Здравствуйте, тов.Тока!

Первым долгом разрешите вас поздравить с 25-годовщиной рабоче-крестьянской Красной Армии. Тока, я пропишу , кто я есть. Я, Шныров Терентий Иванович , проживал в гор.Знаменке в сельхозартели импени 14 лет октября , призван в армия 1.01.42г., где и сейчас нахожусь.Тов.Тока , я 1 сентября выехал на фронт. ...но 2 февраля дрался с немецкими оккупантами , сейчас вы уже слыхали об этих величайших победах под Сталинградом.

Тов.Тока не забывайте о моей семье, помогайте моим сёстрам и братьям, а я буду бить немецких гадов ещё крепче , меня наградили медалью «За боевые заслуги». Я вступил в кандидаты ВКПб , думаю драться коммунистов. Тов.Тока , моя мать мне пишет , что стипендию получает мало , только 12 р. в месяц , мы оба с отцом в армии , работать некому , мать больна. Прошу вас, тов.Тока , не забывайте про семью , тов.Тока , буду ждать ответ и прошу вас не забывайте о фронте , с горячим приветом Шнвров Т.И.

30 июня 1943 г.

Шифрованный текст:

Ыфэзшь фу аьщюл Юрьщюфк Фнлщънфгл Дщжънл.

Упылнэюняхюр, юън.Юъцл!

Ырьнжш пъчюъш ылуърдфюр нлэ ыъупылнфюз э 25-оьпънефщъх ылмъгр-църэюзкщэцъх Цълэщъх Лышфф. Юъцл, к ыъыфдя , цюъ к рэюз. К, Дщжън Юрьщюфх Фнлщънфг , ыъътфнлч н оьъ.Ущлшрщцр н эрчзбъульюрчф фшырщф 14 чрю ыцюкмьк , ыъфунлщ н лышфк 1.01.42о., опр ф эрхглэ щлбътяэз.Юън.Юъцл , к 1 эрщюкмьк нжрблч щл аьщю. ...щъ 2 арнылчк пылчэк э щршрвцфшф ыцяылщюлшф , эрхглэ нж ятр эчжблчф ым июфб нрчфгхдфб ыъмрплб ыъп Эюлчфщюьлпъш. Юън.Юъцл щр улмжнлхюр ь шърх эршзр, ыъшьолхюр шъфш эсэюьлш ф мьлюзкш, л к мяпя мфюз щршрвцфб олпън рес църыгр , шрщк щлюьлпфчф шрплчзй «Ул мърнжр улэчяоф». К нэюяыфч н цлщпфплюж НЦЫм , пашлй пылюзэк цъшшыщфэюън. Юън.Юъцл , шък шлюз шщр ыфдрю , гюъ эюфырщпфй ыъчяглрю шлчъ , юъчзцъ 12 ь. н шрэкв , шж ымл э ыювьш н лышфф , ылмъюлюз щрцъшы , шлюз мъчзщл. Ыъдя нлэ, юън.Юъцл , щр улмжнлхюр ыъ эршзй , юън.Юъцл , мяпя тплюз ыюнрю ф ыъдя нлэ щр улмжнлхюр ь аьщюр , э оьькгфш ыъфнрюъш Дщньън Ю.Ф.

30 фйщк 1943 о.

Задача 7. Шифрование с использованием ключа $k=15$. Буква «Е» «сдвигается» на пятнадцать букв вперёд и становится буквой «У». Твёрдый

знак, перемещённый на пятнадцать букв вперёд, становится буквой «И», и так далее:

Оригинальный текст :

Письмо Героя Советского Союза МИХАИЛА АРТЕМЬЕВИЧА БУХТУЕВА
маме Раисе Семёновне

Письмо писано 2 ноября 1943 года.

Добрый день , весёлый час, здравствуйте , дорогие родители, шлю я вам свой горячий привет – маме, Ване , Марусе , Гоше , Нине, Васе , Толе , Воле. Во-первых строках моего письма я сообщая вам о своей жизни. Живу пока ничего. Сейчас я нахожусь в дороге – еду на запад , на Урал в танковое училище с.Бердска. Выбыл 29 октября. Пока я жил в Бердске от вас ни одного письма не получал, а вам много писал. Фотокарточек не посылал, потому что не приходилось фотографироваться. А ребятам передайте так – когда я уезжал , то все говорили , сто писать письма будут , но , оказывается мне получить не от кого. Пишите чаще письма. Как приеду , то сразу сообщу вам адрес, а сейчас нахожусь в дороге. Передайте по приветам девочкам – Полине , Ире , Кате, Вале и остальным. Ребятам – Алехе, Паше, Кеше , Ивану Ш., Саше Сол., Валентину Ворон., Анатолию и остальным. А также всем мужикам и женщинам от меня по большому приветам.

Я посылаю , мама , тебе справку на получение пособий. Ну, пишите чаще письма. Как приеду , сразу сообщу адрес. Ну, пока до свидания, с приветом ваш сын.

М.Бухтуев.

Шифрованный текст:

Ючакыэ Суяэн Аэрубащэсэ Аэмцо ЫЧДОЧЪО ОЯБУЫКУРЧЁО ПВДБВУРО
ыоыу Яочау Ауыфьэрбу

Ючакыэ ючаоьэ 2 ьэнпян 1943 сэто.

Тэпайш туьк , руафьйш ёоа, цтяорабрвшбу , тэяэсчу яэтчбуьч, жъм н
роы арэш сэянёчш юячруб – ыоыу, Роьу , Ыоявау , Сэжу , Ычьу, Роау , Бэьу ,
Рэьу. Рэ-юуярьд абяэщод ыэусэ ючакыо н аээпзон роы э арэуш хчцьч. Хчрв

юэщо ьчёусэ. Аушёоа н ьодэхвак р тэяэсу – утв ьо цоюот , ьо Вяоъ р боьщэрэу вёчъчзу а.Пуятащо. Рйпйъ 29 эщбнпян. Юэщо н хчъ р Пуятащущэб роа ьч этъэсэ ючакыо ьу юэьвёоъ, о роы ььэсэ ючаоъ. Гэбэщоябэёущ ьу юзайтоъ, юэбэыв ёбэ ьу юячдэтчъэак гэбэсяогчяэробкан. О яупнбоы юуяутошбу бош – щэсто н вуцхоъ , бэ рау сэрэячъч , абэ ючаобк ючакыо пвтвб , ьэ , эщоцйроубан ььу юэьвёчбк ьу эб щэсэ. Ючжчбу ёозу ючакыо. Щощ юячутв , бэ аяоцв аээпзв роы отяуа, о аушёоа ьодэхвак р тэяэсу. Юуяутошбу юэ юячрубв турёобобы – Юэъчъу , Чяу , Щобу, Роъу ч забобъкыйы. Яупнбоы – Оъуду, Юожу, Щужу , Чроъв Ж., Аожу Аэъ., Роъуьбчъв Рэяэъ., Оьобэъчм ч забобъкыйы. О бошху рауы ьвхчщобы ч хуьзчъобы эб ьуьн юэ пэъжэыв юячрубв.

Н юзайъом , ьобыо , бупу аюяорщв ьо юэьвёуьчу юэазпчш. Ъв, ючжчбу ёозу ючакыо. Щощ юячутв , аяоцв аээпзв отяуа. Ъв, юэщо тэ арчтоьчн, а юячрубэы рож айъ.

Ы.Пвдбвур.

Задача 8. Расшифровать текст со сдвигом на 1 букву назад.

Оригинальный текст : «Йётвдудфдхл, ёртрерл уэпрм Фрнб! 22 капб кусрнпбжфуб ерё, мвм б пж дкёжн фжгб. Б рщжпю урумхщкнуб ср фжгж, щвуфр фжгб дусрокпва. Фжгж хиж сбфю нжф, дрф мвмрл фэ грнюърл. Твуфк, уэпрм, гхёю хопжпюмко, нагк удржер гтвфкъмх, хщк жер. Б умртр джтпхую. Дрф стрерпко дужч цвькуфрд, к джтпхую. Мтжсмер шжнха фжгб. Фдрл свсв».

Кй скуюов пжкйджуфпрер урнёвфв.

Ответ : «Здравствуй, дорогой сынок Толя! 22 июня исполняется год, как я не видел тебя. Я очень соскучился по тебе, часто тебя вспоминаю. Тебе уже пять лет, вот какой ты большой. Расти, сынок, будь умненьким, люби своего братишку, учи его. Я скоро вернусь. Вот прогоним всех фашистов, и вернусь. Крепко целую тебя. Твой папа».

Из письма неизвестного солдата.

Задача 9. Расшифровать текст со сдвигом на 5 букв назад

Оригинальный текст : «Ийжуьпе суд, фхнзучужб цйёд п хемршпй.
Жфйхйин 1942 зуи. Лнжн, пеп н д, теийлиуо те жцчхйыш».

«Михежцчжшо, Жйхшцнтбпе н цатшрбпе Винтбпе! Жйхшэьпе, тй
зхшцчн. Зучужбцд п мнсий. Пшфн цатш жерйтпн н цэйо йсш эшэпш. Ргёрг
жец. Ейрпцйо».

Нм фнцйс Ейрпцйд Хузуже, пусетинхе вцпеихнрбн ежнефурпе.
Мжетнй Зйхуд Цужйчцпузу Цугме фуршьнр фуцсйхчту.

Ответ : «Девочка моя, приготовь себя к разлуке. Впереди 1942 год.
Живи, как и я, надеждой на встречу».

«Здравствуй, Верусинька и сынулька Эдинька! Верушечка, не грусти.
Готовься к зиме. Купи сыну валенки и сшей ему шубку. Люблю вас.
Алексей».

Из писем Алексея Рогова, командира эскадрильи авиаполка. Звание
Героя Советского Союза получил посмертно.

Задача 10. Расшифровать текст со сдвигом на 11 букв назад

Оригинальный текст :

Ощлыёф опшж, чщу

Ыщошёп Чкчк, Цийй,

Унщыж у Цпшщвхк!!!

Чуцёп тыщъэуэп, вэщ й мкч эхх ошцнщ шп туькц. Туьжчк мкгу мып
тыщювкц, тк хщэщыёп лщцжгщп ькьюлщ. Уа, чщу ыщошёп, щвпшж чкцщ.
Хкх ащвпэьй тыщвуэкэж м ьмщлщошюи чушюэхю мкгп туьжчпбщ, ок пдп
эххщп, хкх мё тугуэп. Тыщцп эххщнщ туьжчк пдп ьэкшщмугжъй тцпф, пдп
лщцжгп спцкшуй ьопцкэж лщцжгп, луэж ьуцжшпф зёу нкоушю. Ькьюлщ,
чуцёп, тк экхуп туьжчк. Й щвпшж ошмщцпш, оксп шп тшки, хкх тыппокэж
чщи ыкошьэж, вэщ ащэй выппт туьжчк, шщ мё мчпъэп ьщ чшщф.

Хкх ащышгщ, вэщ мё мып чкэпыу, ьпыэьё, лыкэжй, ыщошёп у лцутхуп
мчпъэп ь шкчу хюпэп ь шкчу тыцлою — зэщ пдп щоуш уа эьпа ткццнщм
шкгпф тыцлоё. Хщшпвшщ, скцж ючпыпэж, шщ у м эщсп мыпчй ащвпэьй
ючпыпэж, пыцу эмщй ьчпыэж тыулцутуэ вкь тыцлоё, мё, чщу ыщошёп,

люопэп суэж, ткчпвкэпцжшщ, люопэп щ шкъ ъпэж ткчпвкэпцжшёп ъпъшу у
люопэп ь нщюощ ъщошйэшф нщцщмщф у люопэп нщмщыуэж, вэщ мкг
ыщошщф ёёш, лыкэ, ойой ъщнул вьпэщ м лщыжлп тк ыщоушю, тк
щъмщлщсопшуп.

Чщу чуцёп, чщу опцк ащыщгу. Эщцжхщ окмшщ шп ъщцювкц ъуьпч
щэ Хщцу, ок у ькч окмшщ пчю шп ъуькц.

Хкх чуцёп Мкгу опцк?

Хкх, чкчщвхк, эмщп тощыщмжп?

Ъугуэп лщцжгп у вкдп.

Хыпъхщ бпцюи Мкг Сщык

Ответ :

Добрый день, мои

Родные Мама, Люся,

Игорь и Леночка!!!

Милые простите, что я вам так долго не писал. Письма ваши все получал, за которые большое спасибо. Их, мои родные, очень мало. Как хочется почитать в свободную минутку ваше письмецо, да еще такое, как вы пишете. После такого письма еще становишься злей, еще больше желания сделать больше, бить сильнее эту гадину. Спасибо, милые, за такие письма. Я очень доволен, даже не знаю, как передать мою радость, что хотя через письма, но вы вместе со мной.

Как хорошо, что вы все матери, сестры, братья, родные и близкие вместе с нами куете с нами победу – это еще один их трех залогов нашей победы. Конечно, жаль умереть, но и в тоже время хочется умереть, если твоя смерть приблизит час победы, вы, мои родные, будете жить, замечательно, будете о нас петь замечательные песни и будете с гордо поднятой головой и будете говорить, что ваш родной сын, брат, дядя погиб честно в борьбе за родину, за освобождение.

Мои милые, мои дела хороши. Только давно не получал писем от Коли, да и сам давно ему не писал.

Как милые Ваши дела?

Как, мамочка, твое здоровье?

Пишите больше и чаще.

Крепко целую Ваш Жора

3.2. Задачи модифицированного шифра Цезаря

Задача 11. Оригинальный текст : Паспортные данные (кем выдан)

МП УФМС России по Красноярскому краю и республике Тыва в Сут-Хольском районе

Подставим в соответствие каждой букве её номер в алфавите , а промежутку между словами число 33. Тогда тексту соответствует последовательность чисел:

14,17,21,22,14,19,18,16,19,19,10,10,17,16,12,18,1,19,15,16,33,18,19,12,16,14,21,12,18,1,32,10,18,6,19,17,21,2,13,12,6,20,29,3,1,3,19,21,20,23,16,13,30,19,12,16,14,18,1,11,16,15,6.

Рассмотрим эту последовательность в кольце Z_{33} . Возьмем в этом кольце произвольный обратный элемент , например 3. умножим каждый член этой последовательности на 3:

9,18,30,33,9,24,21,15,24,24,30,30,18,15,3,21,3,24,12,15,33,21,24,3,15,9,30,3,21,3,6,30,21,18,24,18,30,6,6,3,18,30,21,9,3,24,30,30,3,15,6,30,24,3,6,15,21,3,33,15,12,18

Таким образом , текст кодируется в виде :

ЗР ЬЯЗЦ Унцць рн Вувцкняуцвнзь вуве ь урцрьеевр ь Узвц ь Ьвн-Еьцвену увянкp.

Задача 12. Оригинальный текст (сообщение из личной переписки) :

Здравствуйте , я особенно хочу остановиться на вашем предмете , потому что я хочу пойти в медицинский.

Подставим в соответствие каждой букве её номер в алфавите , а промежутку между словами число 33. Тогда тексту соответствует последовательность чисел:

9,5,18,1,3,19,20,3,21,11,20,6 , 33 16,19,16,2,6,15,15,16 23,16,25,21
 16,19,20,1,15,16,3,10,20,28,19,33 15,1 3,1,26,6,14 17,18,6,5,14,6,20,6 ,
 17,16,20,16,14,21 25,20,16 33 23,16,25,21 17,16,11,20,10 3
 14,6,5,10,24,10,15,19,12,10,11.

Рассмотрим эту последовательность в кольце Z_{33} . Возьмем в этом кольце произвольный обратный элемент, например 3. умножим каждый член этой последовательности на 3:

27,15,21,3,9,24,27,9,20,33,27,18 , 1 15,27,15,6,18,7,7,15 3,15,9,30
 15,27,27,3,7,15,9,30,27,18,24,1 7,3 9,3,12,18,9 18,21,18,15,9,18,27,18 ,
 18,15,27,15,9,20 9,27,15 1 3,15,9,30 18,15,33,27,30 9
 9,18,15,30,6,30,13,27,3,30,33.

Таким образом, текст кодируется в виде:

Щнунвщцзтящр, а нщнерёён внзь нщщвёнзыщрца ёв звкрз рурнзрцр,
 рнцнзт зцн а внзь рняць з зрньёьлщвьа.

Задача 13. Выберем ключевое слово, состоящее из различных букв и известное только посылавшему текст и адресату. Например, возьмем слово «ЗАПИСКА» и рассмотрим:

Исходный текст: Наконец после, продолжительного пути, мы доехали до станции Сучан! Здесь я попал, в железнодорожный строительный батальон.

Подставим в соответствие каждой букве её номер в алфавите:

15 1 12 16 15 6 24 17 16 19 13 6 17 18 16 5 16 13 8 10 20 6 13 30 15 16
 4 6 17 21 20 10 14 29 5 16 6 23 1 13 10 5 16 19 20 1 15 24 10 10 19 21
 25 1 15 9 5 6 19 30 33 17 16 17 1 13 3 8 6 13 6 9 15 16 5 16 18 16 8 15 29
 32 11 19 20 18 16 10 20 6 13 30 15 29 11 2 1 20 1 13 30 16 15

Ключ: записка

записказаписказаписказаписказаписказаписказаписка
 записказаписказаписказаписказаписказаписказапи

9 1 17 10 19 12 1 9 1 17 10 19 12 1 9 1 17 10 19 12 1 9 1 17 10 19 12
 1 9 1 17 10 19 12 1 9 1 17 10 19 12 1 9 1 17 10 19 12 1 9 1 17 10 19 12 1 9
 1 17 10 19 12 1 9 1 17 10 19 12 1 9 1 17 10 19 12 1 9 1 17 10 19 12 1 9 1 17
 10 19 12 1 9 1 17 10 19 12 1 9 1 17 10

Сумма : 24 2 29 26 1 18 25 26 17 3 23 25 29 19 25 6 33 23 27 21 15
 14 14 25 2 16 17 26 22 4 20 33 8 6 25 20 4 11 1 3 11 19 20 5 2 20 27 10 14
 7 3 7 19 29 17 26 12 30 13 27 18 14 15 10 32 26 24 28 19 25 9 32 6 18 23
 20 29 19 33 20 6 18 14 6 16 13 21 21 13 21 10 14 17 32

Таким образом , текст кодируется в виде : Цбышари шпвхи
 ысиеяхщфунммчбоп шфгт , яж еиелиюф еи тгйавйс Тдбтщ! Имёвё с
 ыпшкь л щрмниющщъсчзюерхтыс ятермеол уулуимпю.

Задача 14. Выберем ключевое слово ,состоящее из различных букв и
 известное только посылавшему текст и адресату. Например , возьмем слово
 «ПАСПОРТ» и рассмотрим :

Исходный текст: Паспортные данные Кузьменко Иван Петрович :
 Отделом УФМС России по Красноярскому краю в Советском районе город
 Красноярск.

Подставим в соответствие каждой букве её номер в алфавите:

17,1,19,17,16,18,20,15,29,6 5,1,15,15,29,6 12,21,9,30,14,6,15,12,16
 10,3,1,15 17,6,20,18,16,3,10,25 : 16,20,5,6,13,16,14 21,22,14,19
 18,16,19,19,10,10 17,16 12,18,1,19,5,16,33,18,19ву,12в,16,,14,21 12,18,1,32
 3 19,16,3,6,20,19,12,16,14 18,1,11,16,16,6 4,16,18,16,5
 12,18,1,19,15,16,33,18,19,22.

Ключ : паспорт

паспортпаспортпаспортпаспортпаспортпаспортпаспортпаспорт
 паспортпаспортпаспортпаспортпаспортпаспортпаспор

Подставим в соответствие каждой букве её номер в алфавите:

17,1,19,17,16,18,20,17,1,19,17,16,18,20,17,1,19,17,16,18,20,17,1,19,17,16,
 18,20,17,1,19,17,16,18,20,17,1,19,17,16,18,20,17,1,19,17,16,18,20,17,1,19,17,16,

18,20,17,1,19,17,16,18,20,17,1,19,17,16,18,20,17,1,19,17,16,18,20,17,1,19,17,16,
18,20, 17,1,19,17,16,18,20, 17,1,19,17,16,18,20, 17,1,19,17,16,18.

Сумма : 1,2,5,1,32,3,7,32,30,25 22,17,33,2,13,7 31,5,25,15,31,7,1,29,32
28,23,18,16 3,23,3,3,3,20,11 : 33,3,23,26,30,17,33 5,5,32,5 2,17,5,3,3,28 4,33
13,4,18,2,33,3,17,19,5,29,32,32,8 32,2,2,18 20 2,1,23,23,21,5,29,32,32
5,18,12,2 32,22 22,13,2,17,24 29,1,19,6,32,17,19,2,2,30.

Таким образом , текст кодируется в виде

Абдаювёюзи фпяблё эдинэаыюаыю ъхро вхвввти : явхшьпя ддюд
бпеввъ гя лгрбьявпсдыююж юббр т баххудыюю дркб юф фябпу ыасеюпсбб.

Задача 15. Выберем ключевое слово ,состоящее из различных букв и
известное только посылавшему текст и адресату. Например , возьмем слово
«ТУРЧИНЫ» и рассмотрим

Исходный текст : Неужели? Стало быть в тот момент генерал никак не
мог находиться в доме Турчиных.

Подставим в соответствие каждой букве её номер в алфавите:

5,6,21,8,6,13,10 ? 19,20,1,13,16 2,29,20,30 3 20,16,20 14,16,14,6,15,20
4,6,15,6,18,1,13 15,10,12,1,12 15,6 14,16,4 15,1,23,16,5,10,20,30,19,33 3
5,16,14,6 20,21,18,25,10,15,29,23.

Ключ : турчины

Турчинытурчинытурчинытурчинытупчинытурчинытурчиныту
рчинытурч

20,21,18,25,10,15,29, 20,21,18,25,10,15,29, 20,21,18,25,10,15,29,
20,21,18,25,10,15,29, 20,21,18,25,10,15,29, 20,21,18,25,10,15,29,
20,21,18,25,10,15,29, 20,21,18,25,10,15,29, 20,21,18,25,10,15,29, 20,21,18,25.

Сумма :

2,27,6,33,16,28,6 ? 6,8,19,5,26 17,25,7,18 21 12,26,2 10,3,2,24,7,30
19,2,2,27,3,26,23 30,16,32,22,30 7,16 29,12,24 3,19,15,26,20,6,7,18,4,25 13
20,12,1,27 5,13,28,7,6,2,17,8.

Таким образом , текст кодируется в виде:

Бщесое? Еждш пчёр у кшб ивбцеь сббщвхх ьоюфь ёо ыкц
вснштеерги ткащ длъеебпж.

Задача 16. Выберем ключевое слово ,состоящее из различных букв и
известное только посылавшему текст и адресату. Например , возьмем слово
«ВРЕМЯ» и рассмотрим

Исходный текст :

Ещё не поздно спасти положение. Главное – не терять времени. Кто ,
если не мы?

Подставим в соответствие каждой букве её номер в алфавите:

6,27,7 15,6 17,16,9,5,15,16 19,17,1,19,20,10 17,16,13,16,8,6,15,10,6 .
4,13,1,3,15,16,6 – 15,6 20,6,18,33,20,30 3,18,6,14,6,15,10. 12,20,16 ,
6,19,13,10 15,6 14,29?

Ключ : время

Времявремявремявремявремявремявремявремявремявремяврем

3,18,6,14,33, 3,18,6,14,33, 3,18,6,14,33, 3,18,6,14,33, 3,18,6,14,33,
3,18,6,14,33, 3,18,6,14,33, 3,18,6,14,33, 3,18,6,14,33, 3,18,6,14,33, 3,18,6,14,33,
3,18,6,14.

Сумма : 9,12,13 29,6 20,1,15,19,15,19иии4,23,15,19,23,28
23,30,13,19,24,12,29,10,9. 22,19,15,3,18,1,12 – 29,6 23,24,24,14,20,33
21,20,14,9,33,16 . 26,20,19 24,25,27,10 18,24 20,10.

Таким образом, текст кодируется в виде:

Зкл ые танснс гхнсхъ хълсцкылз . Фснврак – ые хццмтя уцтмзйи штс
цищи рц ти?

ЗАКЛЮЧЕНИЕ

В данной выпускной квалификационной работе были рассмотрены теоретические основы кодирования и декодирования личной информации, история возникновения кодирования и декодирования, а также теоретические основы шифра Цезаря. Приведены авторские задачи применение некоторых алгоритмов кодирования и декодирования личной информации с использованием шифр Цезаря.

С глубокой древности люди искали эффективные способы передачи информации:

- Движение факелов использовал древнегреческий историк Полибий (II в. До н.э.);
- Оптический телеграф – семафор – впервые использовал
- Движение электромагнитной стрелки в электромагнитных телеграфных аппаратах впервые применили русский физик П.Л. Шиллинг (1832) и профессора Гёттингенского университета Вебер и Гаусс (1833) и т.д.

Одновременно с потребностью передавать информацию люди искали способы скрыть смысл передаваемых сообщений от посторонних любопытных глаз. Императоры, торговцы, политики и шпионы искали способы шифрования своих посланий.

В выпускной квалификационной работе были рассмотрены такие понятия, как кодер и декодер, код, кодирования и декодирования информации, шифр Цезаря и т.д.

В результате выполнения выпускной квалификационной работы были получены навыки составление задач по некоторым алгоритмам кодирования и декодирования личной информации с использованием шифр Цезаря. Основными методами при решении задач использована метод сдвига, таблица Виженера и модифицированный шифр Цезаря. Всего составлены и решены 16 задач, из них методом сдвига 10 задач с использованием таблицы Виженера, 6 задач методом модифицирования. Составленные задачи полностью выполнены. Закодировали и декодировали такие личные

информации , как паспортные данные, личные фронтовые письма и записки, выписка личного банковского счёта, личные смс сообщения, заключения и выписка врачей. Полученные задачи можно рекомендовать для решения ученикам общеобразовательных школ и других учебных заведений.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. А.В.Косточка . Дискретная математика . Учебное пособие (часть 2). Новосибирск 2001.С.43-52.Загл.с экрана.- URL:<http://www.codingtheory.nsu.ru/literature/kostochka-soloveva.pdf> (дата обращения 17.03.2020).-Текст: электронный.
- 2.А.Г.Коробейников, Ю.А.Гатчин. Математические основы криптологии. Учебное пособие. Санкт-Петербург 2004.С.12-18.
3. А.Д. Пospelов , В.Б.Алексеев. Дискретная математика (II семестр) . Москва 2002.С.32-37.
4. А.И.Митюхин. Теория кодирования .Учебное пособие ,Минск 2014.С4-6.—Загл. с экрана.-URL: <http://sparadise.org/files/arhiv/files/beloruskiy-gosudarstvennyy-universitet-informatiki-i-radioelektroniki/tk/metoda-kniga/uchebnoe-posobie-po-teoriya-kodirovaniya-2075800656-sparadise.org.pdf> (дата обращения: 09.12.2019).-Текст : электронный.
5. А.И.Гусева. Дискретная математика: Учебник. А.И. Гусева, В.С. Киреев, А.Н. Тихомирова. - М.: Курс, 2017. С.245-248.
6. В.Д. Гоппа, Введение в алгебраическую теорию информации / В.Д. Гоппа. - М.: ФИЗМАТЛИТ, 2019. С.56-78.
7. В.И.Донской. Дискретная математика. Симферополь 2000.С.250-256. Интернет исто
8. М.А.Романов. Криптография и защита информации. Учебное пособие. Пинск ПалесГУ 2016.С.8-10.
9. Н.А.Гатченко, А.С.Исаев , А.Д.Яковлев. Криптографическая защита информации. Учебное пособие. Санкт-Петербург 2014.С.28-32.-Загл.с экрана.-URL: <https://books.ifmo.ru/file/pdf/929.pdf> (дата обращения 06.01.2020).Текст : электронный.
10. Н.Ю.Прокопенко. Дискретная математика. Нижний-Новгород 2016.С.87-90.
11. С.Г.Колесников. Дискретная математика .Элементы теория кодирования. Красноярск 2006. С.3-24.

12. С.В.Судоплатов, Е.В.Овчинникова. Дискретная математика. Новосибирск 2011. С.46-50.
- 13.С. И. Чечета, Введение в дискретную теорию информации и кодирования. Учебное пособие / С.И. Чечета. - М.: МЦНМО, 2014. С.130-143.
14. Ф.И.Соловьева. Введение в теорию кодирования. Учебное пособие. Новосибирск 2006.С.20-25.Загл. с экрана.-URL: <http://tc.nsu.ru/uploads/codingtheory.pdf> (дата обращения 14.04.2020). Текст: электронный.
15. Ю.А. Зуев, Современная дискретная математика в задачах и решениях: От перечислительной комбинаторики до криптографии XXI века: Более 700 задач с решениями / Ю.А. Зуев. - М.: Ленанд, 2019. С.278-286.
16. Ю.Н.Мальцев, Введение в дискретную математику. Элементы комбинаторики, теории графов и теории кодирования / Ю.Н. Мальцев, Е.П. Петров. - М.: [не указано], 2017. С.457-480.
17. Ю.Н.Мальцев,Е.П.Петров. Введение в дискретную математику, Барнаул 1997.С.83-92.
18. Я.М.Ерусалимский. Дискретная математика. Теория и практикум: Учебник / Я.М. Ерусалимский. - СПб.: Лань, 2018. С.167-175.